Introduction

Cryptography and Protocols

Andrei Bulatov

Course Info

- **Instructor: Andrei Bulatov**
  - Email: abulatov@sfu.ca
  - Room: TASC 8013
  - Office hours (tentative):
    Wednesday 13:00 – 14:00 (starting Jan 13) ONLINE

- **TAs:**
  - Oleksii Omelchenko, email: oomelche@sfu.ca
  - Jiawen Zhang, email: jiawen_zhang@sfu.ca

- **Course webpage**
  - https://canvas.sfu.ca/courses/69867

Remote instruction

- **Lectures:**
  - Pre-recorded and posted on Canvas
- **Office hours**
  - Live through Zoom. Links will be posted
- **Quizzes and exams**
  - Online on Canvas
- **Hands-on assignments, OpenSSL**
  - Remote access to CSIL

Course Info

- **Books:**

  Cryptography and network security. Principles and practice,
  William Stallings, Pearson, 2014: 6th edition

  Introduction to modern cryptography,
  Jonathan Katz, Yehuda Lindell, Chapman and Hall, 2008

  Handbook of Applied Cryptography,
  Alfred J.Menezes, Paul C. van Oorschot, and
  Scott A. Vanston, CRC-Press, 1996

  Practical Cryptography,
  Niels Ferguson, Bruce Schneier, Wiley Publishing, 2003

Course Info

- **Online Lecture Notes:**

  Bellare-Rogaway's lecture notes

  http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf

  Boneh's lecture notes

  https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/

Course Info

- **Other online resources:**

  Cryptology ePrint archive

  https://eprint.iarch.org

  Wikipedia Cryptography

  https://en.wikipedia.org/wiki/Cryptography

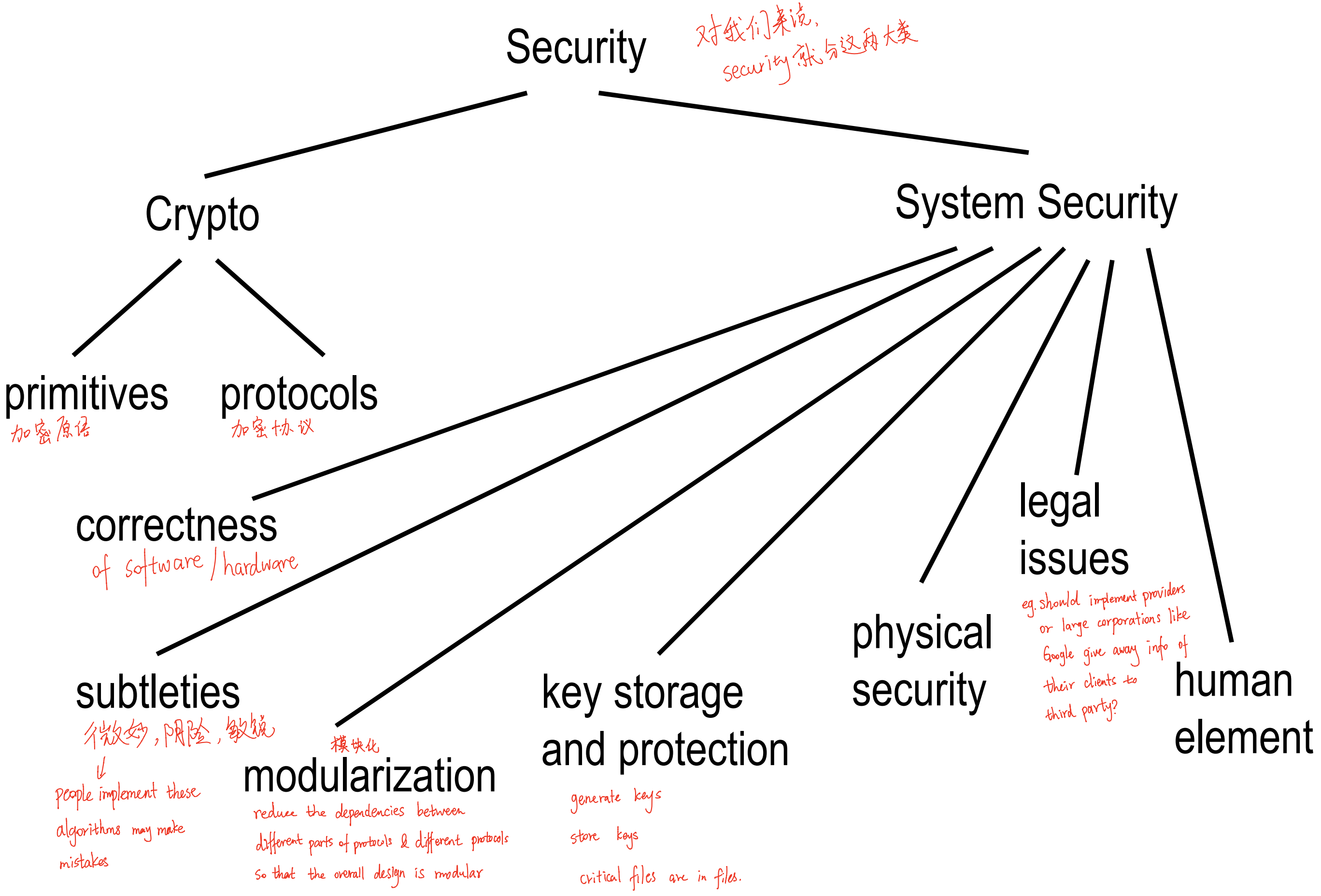
  National Institute of Standards and Technology

  http://csrc.nist.gov/groups/ST/index.html**:**

Course Info

- **Grading:**
  - 5 Assignments (5 × 5%)
  - 4 Quizzes (4 x 10%)
  - 1 Final Exam (1 x 35%)

Security and Cryptography



Security

对我们来说，
security就分这两大类

Crypto

primitives

加密原语

protocols

加密协议

System Security

correctness

of software / hardware

subtleties

微妙，阴险，敏锐

↓

people implement these
algorithms may make
mistakes

模块化

modularization

reduce the dependencies between
different parts of protocols & different protocols
so that the overall design is modular

key storage and protection

generate keys

store keys

critical files are in files.

physical security

legal issues

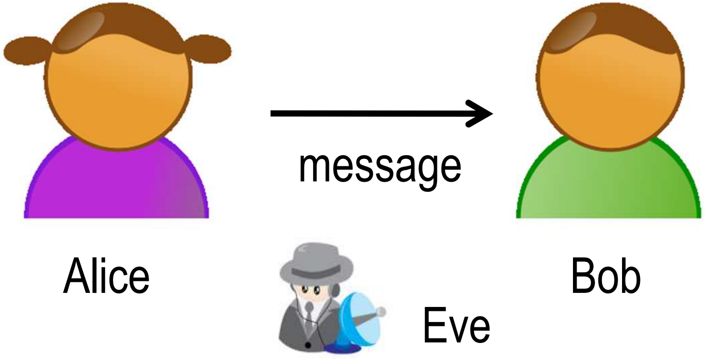
eg. should implement providers
or large corporations like
Google give away info of
their clients to
third party?

human element

Course objective

- What is good security?
- What kind of primitives are there, and what are good primitives?
- How can we construct good protocols from good primitives?

Model of Cryptography: classical



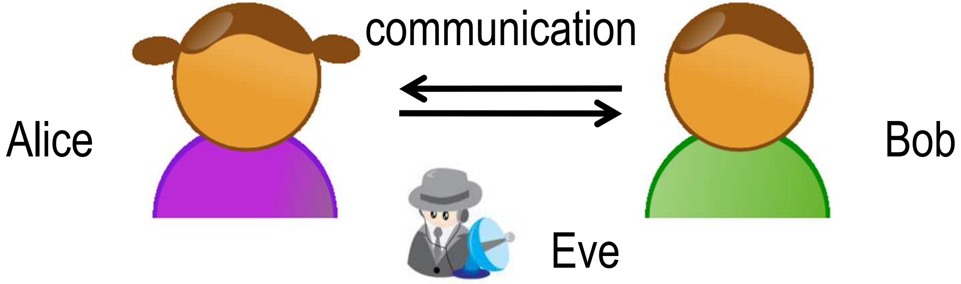
Protocol: a collection of algorithms
(K, E, D)
K – key generation algorithm
E – encryption algorithm
D – decryption algorithm

Goal: privacy

Ideal: ideal channel 理想信道

Eve's capabilities: known ciphertext attack 已知密文攻击

Model of Cryptography: modern



Goals:

- privacy – nobody should understand except the sender & receiver
- authenticity 真实，可靠，– Bob need to make sure the meg is from Alice but nobody else.
- integrity – make sure the msg doesn't change on the way.
- non-repudiation 不可否认性（指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为
- More:
  - e-auctions 电子拍卖
  - online coin flipping
  - zero-knowledge proofs

…

Eve's capabilities:

- known cipher text attack
- known plaintext attack
- chosen plaintext attack
- chosen ciphertext attack

已知密文攻击

已知明文攻击

选择明文攻击

选择密文攻击

Topics

- Historical remarks
- Security: perfect, statistical, and computational
- Pseudo-random generators and stream ciphers
- Pseudo-random functions and authentication
- Block ciphers, DES, AES 分组密码
- Symmetric encryption schemes
- Symmetric authentication schemes, Kerberos
- Public key cryptography, RSA
- Asymmetric encryption schemes
- Key distribution, SSL
- Digital signatures, WEP, PKI
- Zero knowledge
- E-commerce, e-voting, etc.